In re Patent Application of:
POMET ET AL.
Serial No. **09/727,300**
Filing Date: **NOVEMBER 30, 2000**

In the Claims:

Claims 1 to 11 (Cancelled).

12. (Previously Presented) An electronic device comprising:

a central processing unit;

at least one peripheral device;

a data bus connected between said at least one peripheral device and said central processing unit through which data travels at a rate of a clock signal; and

a transmission line connected between said at least one peripheral device and said central processing unit for providing a random signal thereto that is synchronous with the clock signal;

said central processing unit and said at least one peripheral device each comprising a data encryption/decryption cell connected to said data bus and to said transmission line for generating a same current secret key at each clock cycle based upon the random signal.

13. (Previously Presented) An electronic device according to Claim 12, wherein said at least one peripheral device comprises a memory.

14. (Previously Presented) An electronic device according to Claim 12, wherein the same current secret key changes at each successive clock cycle.

In re Patent Application of:
POMET ET AL.
Serial No. **09/727,300**
Filing Date: **NOVEMBER 30, 2000**

15. (Previously Presented) An electronic device according to Claim 12, wherein each data encryption/decryption cell comprises a shift register having an input for receiving the random signal and an input for receiving the clock signal, and an output for providing the same current secret key at each clock cycle.

16. (Previously Presented) An electronic device according to Claim 15, wherein said shift register comprises a feedback type shift register.

17. (Previously Presented) An electronic device according to Claim 15, wherein said shift register performs a polynomial function based upon n most recent values of the random signal.

18. (Previously Presented) An electronic device according to Claim 12, wherein each data encryption/decryption cell comprises:

an encryption module having an input for receiving the secret key and an input for receiving the data to be transmitted, and an output for providing encrypted data; and

a decryption module having an input for receiving the secret key and an input for receiving the data, and an output for providing decrypted data.

19. (Previously Presented) An electronic device according to Claim 18, wherein the data encryption/decryption

cell of said central processing unit further comprises a conditional circuit for applying the secret key or a neutral key to said encryption and decryption modules based upon an encryption enabling signal.

20. (Previously Presented) An electronic device according to Claim 19, further comprising a peripheral access control circuit connected to said central processing unit and said at least one peripheral device for generating the encryption enabling signal based upon an address of said at least at least one peripheral device.

21. (Previously Presented) An electronic device according to Claim 18, wherein said encryption module and said decryption module each operate based upon a same mathematical function.

22. (Previously Presented) An electronic device according to Claim 12, further comprising a random signal generator connected to said transmission line for generating the random signal that is synchronous with the clock signal, and wherein said random signal generator further comprises a consumption masking circuit.

23. (Previously Presented) An electronic device according to Claim 22, wherein said random signal generator comprises a D-type flip-flop having an input for receiving a random binary signal and an input for receiving the clock signal,

and an output for providing the random signal; and wherein said consumption masking circuit is connected between the output of said D-type flip-flop circuit and said transmission line.

24. (Previously Presented) An electronic device according to Claim 22, wherein a value of the same current secret key on said transmission line is set to zero by default by said central processing unit, and said random signal generator comprises a logic circuit to transmit the random signal on said transmission line after activation of a control signal by said central processing unit.

25. (Previously Presented) An electronic device comprising:

a central processing unit;

at least one memory device;

a data bus connecting said at least one memory device and said central processing unit; and

a transmission line connecting said at least one memory device and said central processing unit for providing a random signal thereto that is synchronous with a clock signal;

said central processing unit and said at least one memory device each comprising a data encryption/decryption cell connected to said data bus and to said transmission line for generating a same current secret key at each cycle of the clock signal based upon the random signal.

26. (Previously Presented) An electronic device

according to Claim 25, wherein each data encryption/decryption cell comprises a shift register having an input for receiving the random signal and an input for receiving the clock signal, and an output for providing the same current secret key at each cycle of the clock signal.

27. (Previously Presented) An electronic device according to Claim 26, wherein said shift register performs a polynomial function based upon n most recent values of the random signal.

28. (Previously Presented) An electronic device according to Claim 25, wherein each data encryption/decryption cell comprises:

an encryption module having an input for receiving the secret key and an input for receiving the data to be transmitted, and an output for providing encrypted data; and

a decryption module having an input for receiving the secret key and an input for receiving the data, and an output for providing decrypted data.

29. (Previously Presented) An electronic device according to Claim 28, wherein the data encryption/decryption cell of said central processing unit further comprises a conditional circuit for applying the secret key or a neutral key to said encryption and decryption modules based upon an encryption enabling signal.

30. (Previously Presented) An electronic device according to Claim 29, further comprising a memory access control circuit connected to said central processing unit and said at least one memory device for generating the encryption enabling signal based upon an address of said at least at least one memory device.

31. (Previously Presented) An electronic device according to Claim 28, wherein said encryption module and said decryption module each operate based upon a same mathematical function.

32. (Previously Presented) An electronic device according to Claim 25, further comprising a random signal generator connected to said transmission line for generating the random signal that is synchronous with the clock signal, and wherein said random signal generator further comprises a consumption masking circuit.

33. (Previously Presented) An electronic device according to Claim 25, wherein said random signal generator comprises a D-type flip-flop having an input for receiving a random binary signal and an input for receiving the clock signal, and an output for providing the random signal; and wherein said consumption masking circuit is connected between the output of said D-type flip-flop circuit and said transmission line.

34. (Previously Presented) A smart card comprising:

a central processing unit;

at least one peripheral device;

a data bus connecting said at least one peripheral device and said central processing unit;

a transmission line connecting said at least one peripheral device and said central processing unit; and

a random signal generator connected to said transmission line for generating a random signal thereon that is synchronous with a clock signal;

said central processing unit and said at least one peripheral device each comprising a data encryption/decryption cell connected to said data bus and to said transmission line for generating a same current secret key at each cycle of the clock signal based upon the random signal.

35. (Previously Presented) A smart card according to Claim 34, wherein each data encryption/decryption cell comprises a shift register having an input for receiving the random signal and an input for receiving the clock signal, and an output for providing the same current secret key at each cycle of the clock signal.

36. (Previously Presented) A smart card according to Claim 35, wherein said shift register performs a polynomial function based upon n most recent values of the random signal.

37. (Previously Presented) A smart card according to Claim 34, wherein each data encryption/decryption cell comprises:

an encryption module having an input for receiving the secret key and an input for receiving the data to be transmitted, and an output for providing encrypted data; and

a decryption module having an input for receiving the secret key and an input for receiving the data, and an output for providing decrypted data.

38. (Previously Presented) A smart card according to Claim 37, wherein the data encryption/decryption cell of said central processing unit further comprises a conditional circuit for applying the secret key or a neutral key to said encryption and decryption modules based upon an encryption enabling signal.

39. (Previously Presented) A smart card according to Claim 38, further comprising a peripheral access control circuit connected to said central processing unit and said at least one peripheral device for generating the encryption enabling signal based upon an address of said at least at least one peripheral device.

40. (Previously Presented) A smart card according to Claim 37, wherein said encryption module and said decryption module each operate based upon a same mathematical function.

41. (Previously Presented) A smart card according to Claim 34, wherein said random signal generator comprises a D-type flip-flop having an input for receiving a random binary signal and an input for receiving the clock signal, and an output for

providing the random signal; and wherein said consumption masking circuit is connected between the output of said D-type flip-flop circuit and said transmission line.

42. (Previously Presented) A method for exchanging data in an electronic device comprising a central processing unit and at least one peripheral device, a data bus connected between the at least one peripheral device and the central processing unit, and a transmission line connected between the at least one peripheral device and the central processing unit, the method comprising:

providing a random signal to the central processing unit and to the at least one peripheral device; and

generating a same current secret key at each cycle of a clock signal based upon the random signal in the central processing unit and the at least one peripheral device.

43. (Previously Presented) A method according to Claim 42, wherein the at least one peripheral device comprises a memory device.

44. (Previously Presented) A method according to Claim 42, wherein each data encryption/decryption cell comprises a shift register having an input for receiving the random signal and an input for receiving the clock signal, and an output for providing the same current secret key at each cycle of the clock signal.

45. (Previously Presented) A method according to Claim 44, wherein the shift register performs a polynomial function based upon n most recent values of the random signal.

46. (Previously Presented) A method according to Claim 42, wherein each data encryption/decryption cell comprises:

an encryption module having an input for receiving the secret key and an input for receiving the data to be transmitted, and an output for providing encrypted data; and

a decryption module having an input for receiving the secret key and an input for receiving the data, and an output for providing decrypted data.

47. (Previously Presented) A method according to Claim 46, wherein the data encryption/decryption cell of the central processing unit further comprises a conditional circuit for applying the secret key or a neutral key to the encryption and decryption modules based upon an encryption enabling signal.

48. (Previously Presented) A method according to Claim 47, further comprising a peripheral access control circuit connected to the central processing unit and the at least one peripheral device for generating the encryption enabling signal based upon an address of the at least at least one peripheral device.

In re Patent Application of:
POMET ET AL.
Serial No. **09/727,300**
Filing Date: **NOVEMBER 30, 2000**

49. (Previously Presented) A method according to Claim 42, wherein the random signal is generated by a random signal generator connected to the transmission line.